Computer Safety and Reliability

Ensuring that computer-controlled systems operate safely

Use of computers in safety-critical control systems is becoming prevalent. In the last decade, designers have begun to use computers extensively in applications where personal injury or environmental damage could result if the computer system does not perform as intended. Failure of a critical computer system design to meet safety requirements can lead to significant economic loss, injury, or death. For instance, the reliability of a system that controls a nuclear power plant protection system, or determines the orbit of a space shuttle, is much more critical than that of a system that tracks warehouse inventory. Critical applications require highly reliable computer systems that have a known set of acceptable failure modes.

Evaluation tools to ensure safety

System designers and users are only beginning to understand the unique problems posed by the use of computers in safety and environmentally critical applications. The technology is relatively new, and the "state of the art" continues to change rapidly. Industry needs effective tools to evaluate such systems, including appropriate design codes and standards, analytical techniques, design methods, and computer-aided design systems.

APPLICATIONS

- *Nuclear reactor safety*
- *Pharmaceutical manufacturing*
- *Autonomous vehicles*
- *Chemical process control*
- *Aerospace flight*
- *Environmental control*

LLNL's Computer Safety and Reliability (CS&R) Group is developing such tools to assist the U.S. Nuclear Regulatory Commission in the evaluation of reactor safety systems that use computers, and to assist Department of Energy facilities in the design of safety and environmentally critical computer systems. The products of this effort include review guidance, analytical tools, and assessment tools. The CS&R Group's tools and capabilities can be adapted to other safety-critical or environmental computer applications.

LLNL has applied these tools to assist the NRC in evaluating the safety of advanced nuclear power plant designs. The CS&R Group has been deeply involved in design certification reviews of computer-based protection systems for the four advanced light water reactors designed by U.S. companies. We are also supporting assessments of facilities in Asia and Europe and are participating in the development of domestic and international standards for computers in safety-critical systems.

Areas of expertise

The CS&R Group's areas of expertise include:

Review Criteria
- Data communications
- Programmable logic controllers
- Software reliability
- Off-the-shelf software

Analytical Tools
- Defense-in-depth and diversity analysis
- Complexity analysis
- Safety kernel
- Hazards analysis library

Assessment Tools
- Verification and validation program criteria
- Computer-aided verification and validation program evaluation.

Availability: Our CS&R Group is available now to work with outside partners in further developing and applying our computer safety and reliability expertise.

Contact

Gary Johnson
Phone: (510) 423-8834
Fax: (510) 433-9913
E-mail: johnson27@llnl.gov
Mail code: L-632